

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-213554

(43)Date of publication of application : 06.08.1999

(51)Int.Cl.

G11B 20/10
G06F 12/14
G09C 5/00
H04L 9/32

(21)Application number : 10-291968

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 14.10.1998

(72)Inventor : KATO TAKEHISA
KATO HIROSHI
ENDO NAOKI
YAMADA HISASHI
ENDO KENJIRO

(30)Priority

Priority number : 09361981 Priority date : 20.11.1997 Priority country : JP

(54) COPY PREVENTING DEVICE

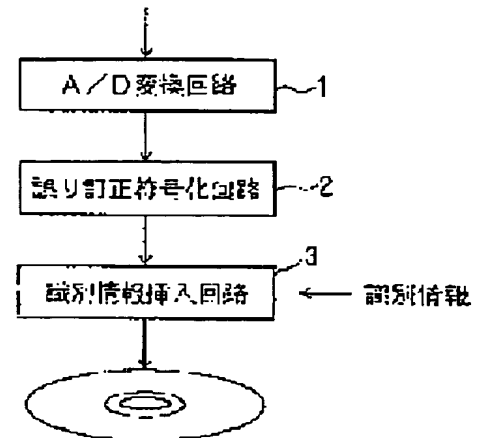
(57)Abstract:

PROBLEM TO BE SOLVED: To prevent unauthorized copy by recording an identification signal expressing whether contents recorded on an information record medium are original or not in an error-correcting code.

SOLUTION: Multimedia data (analog contents) are digitized through procedures of a sampling and quantization. Thereafter, the digital data are subjected to an error-correcting coding in an error-correcting coding circuit 2 in order to correct an error to be generated in a transmission path. Then, an identification signal expressing whether a disk (information recording medium) is original or not is inserted into the digital data subjected to the error-correcting coding in an identification information inserting circuit 3. In this insertion, specific symbols of analog contents and the identification information are replaced and the analog contents into which the identification information are inserted are recorded on the information recording medium.

ディスク製作 # 1

アナログ・コンテンツ



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-213554

(43) 公開日 平成11年(1999) 8月6日

(51) Int.Cl.⁹
G 1 1 B 20/10
G 0 6 F 12/14
G 0 9 C 5/00
H 0 4 L 9/32

識別記号

3 2 0

F I

G 1 1 B 20/10

G 0 6 F 12/14

G 0 9 C 5/00

H 0 4 L 9/00

H

3 2 0 E

6 7 3 Z

審査請求 未請求 請求項の数13 O L (全 23 頁)

(21) 出願番号 特願平10-291968
(22) 出願日 平成10年(1998)10月14日
(31) 優先権主張番号 特願平9-361981
(32) 優先日 平9(1997)11月20日
(33) 優先権主張国 日本 (J P)

(71) 出願人 000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72) 発明者 加藤 岳久
東京都府中市東芝町1番地 株式会社東芝
府中工場内
(72) 発明者 加藤 拓
東京都府中市東芝町1番地 株式会社東芝
府中工場内
(72) 発明者 遠藤 直樹
東京都府中市東芝町1番地 株式会社東芝
府中工場内
(74) 代理人 弁理士 鈴江 武彦 (外6名)

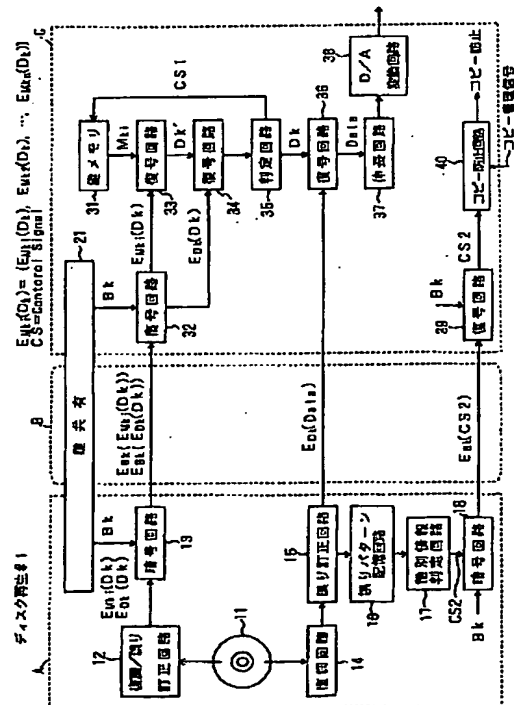
最終頁に続く

(54) 【発明の名称】 コピー防止装置

(57) 【要約】

【課題】 識別情報を誤り訂正符号に記録しておき、この識別情報をもとに不正なコピーを防止する。

【解決手段】 本発明は、暗号化されたデジタルデータを得る暗号化デジタルデータ獲得部(15)と、暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出部(15)と、検出された誤り位置及び誤りシンボル値に基づいて、オリジナルか否かを示す識別情報を検出する識別情報検出部(16)と、検出された識別情報に基づいて、コピーを防止するか否かを決定する決定部(17)と、決定結果に基づいて、情報記録媒体のコピーを防止するコピー防止部(40)とを具備するコピー防止装置である。



【特許請求の範囲】

【請求項1】 暗号化及び誤り訂正符号化されたデジタルデータ、前記暗号化及び誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び誤り訂正符号化されたデジタルデータを復調する第1の復調手段と、前記第1の復調手段により復調された前記暗号化及び誤り訂正符号化されたデジタルデータに誤り訂正処理を行なうことにより暗号化されたデジタルデータを得る暗号化デジタルデータ獲得手段と、前記暗号化デジタルデータ獲得手段による誤り訂正処理により得られる前記暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、前記検出手段により検出された誤り位置及び誤りシンボル値に基づいて、前記暗号化及び誤り訂正符号化されたデジタルデータに前記暗号化及び誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置。

【請求項2】 前記情報記録媒体から前記鍵情報を復号する第1の復号手段と、前記第1の復号手段により復号された鍵情報に基づいて、前記暗号化デジタルデータ獲得手段によって獲得された暗号化されたデジタルデータからデジタルデータを復号する第2の復号手段と、前記第2の復号手段により復号されたデジタルデータを再生する再生手段とをさらに具備することを特徴とする請求項1記載のコピー防止装置。

【請求項3】 前記決定手段は、決定結果を示す制御信号を暗号化して出力し、前記コピー防止手段は、前記制御信号を復号し、この復号された制御信号に基づいてコピーを防止することを特徴とする請求項1記載のコピー防止装置。

【請求項4】 前記識別情報は、誤り訂正符号化された後のデジタルデータのうち、所定のシンボルと置き換えられることを特徴とする請求項1記載のコピー防止装置。

【請求項5】 前記決定手段は、前記識別情報検出手段により検出された識別情報をカウントするカウント手段と、前記カウント手段によりカウントされた識別情報の数が所定の値を超えているか否かを判定する判定手段と、前記判定手段による判定結果に基づいて、コピーを防止するか否かを決定する決定手段とを具備することを特徴

とする請求項1記載のコピー防止装置。

【請求項6】 前記決定手段は、前記識別情報検出手段により検出された識別情報の位置情報に基づいて、コピーを防止するか否かを決定することを特徴とする請求項1記載のコピー防止装置。

【請求項7】 前記決定手段は、決定結果を示す制御信号を乱数を使用して所定の演算を行うことにより第1の制御信号に変換する第1の変換手段と、前記第1の変換手段により変換された第1の制御信号を暗号化する第1の暗号化手段と、前記乱数を暗号化する第2の暗号化手段とを具備し、前記コピー防止手段は、前記第1の暗号化手段により暗号化された第1の制御信号を復号する第1の復号手段と、前記第2の暗号化手段により暗号化された乱数を復号する第2の復号手段と、前記第1の復号手段により復号された第1の制御信号を、前記第2の復号手段により復号された乱数を使用して前記所定の演算を行うことにより、前記制御信号に変換する第2の変換手段と、前記第2の変換手段により変換された制御信号に基づいてコピーを防止する手段とを具備することを特徴とする請求項1記載のコピー防止装置。

【請求項8】 前記識別情報は誤り訂正符号であり、前記識別情報検出手段は、検出された識別情報を誤り訂正符号の誤り訂正能力を利用して訂正することを特徴とする請求項1記載のコピー防止装置。

【請求項9】 暗号化及び積符号により誤り訂正符号化されたデジタルデータ、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータを復調する第1の復調手段と、前記第1の復調手段により復調された前記暗号化及び積符号により誤り訂正符号化されたデジタルデータに外符号の誤り訂正処理を行なうことにより暗号化及び内符号により誤り訂正符号化されたデジタルデータを獲得する第1の獲得手段と、前記第1の獲得手段による誤り訂正処理において得られる前記暗号化及び内符号により誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、前記検出手段により検出された誤り位置及び誤りシンボル値に基づいて、前記暗号化及び内符号により誤り訂正符号化されたデジタルデータに前記暗号化及び内符号により誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、前記識別情報検出手段により検出された識別情報に基づ

いて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置。

【請求項10】 暗号化及び積符号により誤り訂正符号化されたデジタルデータ、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータを復調する第1の復調手段と、

前記第1の復調手段により復調された前記暗号化及び積符号により誤り訂正符号化されたデジタルデータに外符号の誤り訂正処理を行なうことにより暗号化及び内符号により誤り訂正符号化されたデジタルデータを獲得する第1の獲得手段と、

前記第1の獲得手段による誤り訂正処理により得られる暗号化及び内符号により誤り訂正符号化されたデジタルデータにおける第1の誤り位置及び第1の誤りシンボル値を検出する第1の検出手段と、

前記第1の獲得手段により得られた前記暗号化及び内符号により誤り訂正符号化されたデジタルデータに内符号による誤り訂正処理を行なうことにより暗号化されたデジタルデータを復調する第2の復調手段と、

前記第2の復調手段による誤り訂正処理により得られる暗号化されたデジタルデータにおける第2の誤り位置及び第2の誤りシンボル値を検出する第2の検出手段と、前記第1の検出手段により検出された第1の誤り位置及び第1の誤りシンボル値、前記第2の検出手段により検出された第2の誤り位置及び第2の誤りシンボル値に基づいて、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータに前記暗号化及び積符号により誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、

前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置。

【請求項11】 暗号化及び積符号により誤り訂正符号化されたデジタルデータ、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータを復調する第1の復調手段と、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータに前記暗号化及び積符号により誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報のパターンに基づいて、前記第1の復調手段により復調された前記暗号化及

び積符号により誤り訂正符号化されたデジタルデータにおける識別情報を検出する識別情報検出手段と、

前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置。

【請求項12】 暗号化及び誤り訂正符号化されたデジタルデータ、前記暗号化及び誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び誤り訂正符号化されたデジタルデータを復調する第1の復調手段と、

前記第1の復調手段により復調された前記暗号化及び誤り訂正符号化されたデジタルデータに誤り訂正処理を行なうことにより暗号化されたデジタルデータを復調する暗号化デジタルデータ獲得手段と、

前記暗号化デジタルデータ獲得手段による誤り訂正処理により得られる前記暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、

前記暗号化デジタルデータ獲得手段により得られた暗号化されたデジタルデータを復号することによりデジタルデータを復号する復号手段と、

前記復号手段により得られたデジタルデータに透かし情報として埋め込まれた識別情報の位置情報を抽出する抽出手段と、

前記検出手段により検出された誤り位置及び誤りシンボル値、前記抽出手段により抽出された識別情報の位置情報に基づいて、前記暗号化及び誤り訂正符号化されたデジタルデータに前記暗号化及び誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、コピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置。

【請求項13】 暗号化及び誤り訂正符号化されたデジタルデータ、前記暗号化及び誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び誤り訂正符号化されたデジタルデータを復調する第1の復調手段と、

前記第1の復調手段により復調された前記暗号化及び誤り訂正符号化されたデジタルデータに誤り訂正処理を行なうことにより暗号化されたデジタルデータを復調する暗号化デジタルデータ獲得手段と、

前記暗号化デジタルデータ獲得手段による誤り訂正処理により得られる前記暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、

前記情報記録媒体に格納された暗号化された鍵情報を圧縮する圧縮手段と、

前記圧縮手段により圧縮された鍵情報、前記検出手段により検出された誤り位置及び誤りシンボル値に基づいて、識別情報を抽出する抽出手段と、

前記抽出手段により抽出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、

前記決定手段による決定結果に基づいて、コピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、記録媒体上に記録されたマルチメディア・データが、オリジナルなものであるのか、コピーされたものであるのかを判定し、コピーされたものである媒体からの再生であると判定された場合には、コピーを禁止するなどして、不正なコピーを防止するコピー防止装置に関する。

【0002】

【従来の技術】従来、DAT(Digital Audio Tape)やMD(Mini Disc)のようなデジタル記録媒体においては、オリジナルなものからであれば一度限りのデジタル・コピーが可能である。しかし、コピーされたものからの再度のコピー(孫コピー)を作成することはできないようになっている。

【0003】このシステムを、CGMS(Copy Generation Management System)やSCMS(Single Copy Management System)と呼ぶ。これらは、コピーされたものか否か(コピー可能か否か)を、2ビットのフラグで示すものである。

【0004】

【発明が解決しようとする課題】しかし、このようなCGMSやSCMSは、伝送途中で改竄をうけ、不正コピーされる場合があり、不正にコピーされた、一般に海賊版と呼ばれる媒体が流通する、という問題が有る。

【0005】上述したように、従来の不正コピー防止手段では、伝送途中で改竄をうけ、不正コピーされる場合があり、不正にコピーされた、一般に海賊版と呼ばれる媒体が流通する、という問題がある。

【0006】

【課題を解決するための手段】本発明は、上記実情に鑑みてなされたものであり、情報記録媒体に記録されたコンテンツが、オリジナルのものであるか否かを示す識別情報を誤り訂正符号に記録しておき、この識別情報をもとに不正なコピーを防止するコピー防止装置を提供することを目的とする。

【0007】したがって、まず、本発明の第1の発明によれば、暗号化及び誤り訂正符号化されたデジタルデータ、前記暗号化及び誤り訂正符号化されたデジタルデータの暗号化された鍵情報が記録された情報記録媒

体から、前記暗号化及び誤り訂正符号化されたデジタルデータを復調する第1の復調手段と、前記第1の復調手段により復調された前記暗号化及び誤り訂正符号化されたデジタルデータに誤り訂正処理を行なうことにより暗号化されたデジタルデータを得る暗号化デジタルデータ獲得手段と、前記暗号化デジタルデータ獲得手段による誤り訂正処理により得られる前記暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、前記検出手段により検出された誤り位置及び誤りシンボル値に基づいて、前記暗号化及び誤り訂正符号化されたデジタルデータに前記暗号化及び誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置、である。

【0008】また、本発明の第2の発明によれば、暗号化及び積符号により誤り訂正符号化されたデジタルデータ、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータを復調する第1の復調手段と、前記第1の復調手段により復調された前記暗号化及び積符号により誤り訂正符号化されたデジタルデータに外符号の誤り訂正処理を行なうことにより暗号化及び内符号により誤り訂正符号化されたデジタルデータを獲得する第1の獲得手段と、前記第1の獲得手段による誤り訂正処理において得られる前記暗号化及び内符号により誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、前記検出手段により検出された誤り位置及び誤りシンボル値に基づいて、前記暗号化及び内符号により誤り訂正符号化されたデジタルデータに前記暗号化及び内符号により誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置、である。

【0009】さらに、本発明の第3の発明によれば、暗号化及び積符号により誤り訂正符号化されたデジタルデータ、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータを復調する第1の復

調手段と、前記第1の復調手段により復調された前記暗号化及び積符号により誤り訂正符号化されたデジタルデータに外符号の誤り訂正処理を行なうことにより暗号化及び内符号により誤り訂正符号化されたデジタルデータを獲得する第1の獲得手段と、前記第1の獲得手段による誤り訂正処理により得られる暗号化及び内符号により誤り訂正符号化されたデジタルデータにおける第1の誤り位置及び第1の誤りシンボル値を検出する第1の検出手段と、前記第1の獲得手段により得られた前記暗号化及び内符号により誤り訂正符号化されたデジタルデータに内符号による誤り訂正処理を行なうことにより暗号化されたデジタルデータを得る第2の獲得手段と、前記第2の獲得手段による誤り訂正処理により得られる暗号化されたデジタルデータにおける第2の誤り位置及び第2の誤りシンボル値を検出する第2の検出手段と、前記第1の検出手段により検出された第1の誤り位置及び第1の誤りシンボル値、前記第2の検出手段により検出された第2の誤り位置及び第2の誤りシンボル値に基づいて、前記暗号化及び誤り訂正符号化されたデジタルデータに前記暗号化及び積符号により誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置、である。

【0010】さらに、本発明の第4の発明によれば、暗号化及び積符号により誤り訂正符号化されたデジタルデータ、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータを復調する第1の復調手段と、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータに前記暗号化及び積符号により誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報のパターンに基づいて、前記第1の復調手段により復調された前記暗号化及び積符号により誤り訂正符号化されたデジタルデータにおける識別情報を検出する識別情報検出手段と、前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置、である。

【0011】さらに、本発明の第5の発明によれば、暗号化及び誤り訂正符号化されたデジタルデータ、前記暗号化及び誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び誤り訂正符号化されたデジタルデータを復

調する第1の復調手段と、前記第1の復調手段により復調された前記暗号化及び誤り訂正符号化されたデジタルデータに誤り訂正処理を行なうことにより暗号化されたデジタルデータを得る暗号化デジタルデータ獲得手段と、前記暗号化デジタルデータ獲得手段による誤り訂正処理により得られる前記暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、前記暗号化デジタルデータ獲得手段により得られた暗号化されたデジタルデータを復号することによりデジタルデータを得る復号手段と、前記復号手段により得られたデジタルデータに透かし情報として埋め込まれた識別情報の位置情報を抽出する抽出手段と、前記検出手段により検出された誤り位置及び誤りシンボル値、前記抽出手段により抽出された識別情報の位置情報に基づいて、前記暗号化及び誤り訂正符号化されたデジタルデータに前記暗号化及び誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、コピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置、である。

【0012】さらに、本発明の第6の発明によれば、暗号化及び誤り訂正符号化されたデジタルデータ、前記暗号化及び誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び誤り訂正符号化されたデジタルデータを復調する第1の復調手段と、前記第1の復調手段により復調された前記暗号化及び誤り訂正符号化されたデジタルデータに誤り訂正処理を行なうことにより暗号化されたデジタルデータを得る暗号化デジタルデータ獲得手段と、前記暗号化デジタルデータ獲得手段による誤り訂正処理により得られる前記暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、前記情報記録媒体に格納された暗号化された鍵情報を圧縮する圧縮手段と、前記圧縮手段により圧縮された鍵情報、前記検出手段により検出された誤り位置及び誤りシンボル値に基づいて、識別情報を抽出する抽出手段と、前記抽出手段により抽出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、コピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置、である。

【0013】

【発明の実施の形態】以下、本発明の実施形態を図面を用いて説明する。

【0014】本実施形態においては、情報記録媒体は、HDやDVD-RAMなどの記録再生可能な媒体を意味する。また、本実施形態においては、元となる画像や音声などの

マルチメディア・データが、アナログ・データであるものとする。

【0015】<第1の実施の形態>図1は、本発明の第1の実施形態におけるコピー防止装置において使用されるディスクの制作の過程を説明するための図である。

【0016】アナログデータであるマルチメディア・データ（アナログ・コンテンツ）は、A/D変換回路1にて標準化や量子化の手順を経て、ディジタル化される。その後、伝送路中に発生する誤りを訂正するために、誤り訂正符号化回路2にて誤り訂正符号化される。

【0017】誤り訂正符号化については、「符号理論」宮川、岩垂、今井共著 昭晃堂に詳しい。誤り訂正符号化されたディジタル・データには、ディスク（情報記録媒体）がオリジナルであるか否かを示す識別情報が識別情報挿入回路3にて挿入される。

【0018】ここでの挿入は、図2に示すように、特定のアナログコンテンツのシンボルと識別情報とが置き換えられるものである。そして、識別情報が挿入されたアナログコンテンツが情報記録媒体に記録される。図2では、データ部のシンボルのm番目からn番目のシンボルが、それぞれ識別情報 DI_0, \dots, DI_j に入れ替えられる例を示している。

【0019】なお、図2に示した例においては、連続するシンボルのパターンが識別情報と置き換えられているが、ある特定のシンボルを識別情報と置き換えても良いし、連続するシンボルではなく何シンボルか空けたシンボル（例えば1シンボル空けて）を識別情報と置き換えてもよい。

【0020】またデータ部だけでなく、パリティ部のシンボルと入れ替えても構わない。ただし、入れ替えるシンボル数は訂正能力の限界を超えてはならず、訂正能力に余裕を持たせるようにした方が望ましい。

【0021】次に、誤り訂正符号の特定シンボルが識別情報に入れ替えられたディスクの再生について説明する。

【0022】図3は、本発明の第1の実施の形態に係る装置を示す図である。

【0023】なお、DVD(Digital Video Disc, Digital Versatile Disc)には、すでに不正コピー防止のための暗号技術が導入されている。これらの技術については、「DVD 著作権保護システム」館林、松崎、石原、福島、映像情報メディア学会技術報告、1997.5.22, P.15-19、または「DVD、パソコン載る」日経エレクトロニクス、1997.8.18(no.696), p.110-120、に詳細に述べられている。本実施形態においては、概保護技術の説明を省略する。

【0024】文献に依れば、DVDでは三種の暗号鍵を用いてコンテンツを保護しているが、本実施形態では説明の簡略化のために、2つの暗号鍵を用いて説明する。もちろん、1種だけの暗号鍵、3種以上の複数の暗号鍵、

であったとしても、本実施の形態を適用することができる。

【0025】図3において、AはDVDディスクドライブ、Bはバスインターフェース、Cは、例えば画像であればMPEG2復号ユニットのような復号ユニットである。

【0026】DVDディスク11から、暗号化された鍵情報である $EMki(Dk)$ と $EDk(Dk)$ が読み出される。そして、復調/誤り訂正回路12によって、読み出された暗号化された鍵情報 $EMki(Dk)$ と $EDk(Dk)$ の復調、誤り訂正処理が行われる。

【0027】暗号化された鍵情報 $EMki(Dk)$ と $EDk(Dk)$ 以外の暗号化されたコンテンツ情報 $EDk(Data)$ は、復調回路14によって復調される。

【0028】一時暗号鍵 Bk は、鍵共有プロトコル21にてDVDディスクドライブAと復号ユニットC間で共有される。

【0029】一時暗号鍵 Bk を共有したら、暗号化された鍵情報 $EMki(Dk)$ と $EDk(Dk)$ を一時暗号鍵 Bk で暗号化回路13にて暗号化し、 $EBk(EMki(Dk))$ と $EBk(EDk(Dk))$ とを復号ユニットCへ送る。

【0030】さて、復号ユニットCの復号回路32では、 $EBk(EMki(Dk))$ と $EBk(EDk(Dk))$ を共有した一時暗号鍵 Bk を用いて復号する。そして、鍵メモリ31に納められたn個のマスタ鍵 $Mki(i=1, \dots, n)$ を順次呼び出し、 $EMki(Dk)$ を復号回路33にて復号する。

【0031】復号回路33による復号の結果得られた Dk' を復号鍵として、復号回路34にて $EDk(Dk)$ を復号する。そして、復号回路34による復号により得られた結果と復号回路33による復号の結果得られた Dk' とを判定回路35で比較し、一致すれば Dk を暗号化したマスタ鍵を特定でき、かつデータを暗号化した暗号鍵 Dk を得られる。一致しなければ、制御信号 $CS1$ にて鍵メモリから新たなマスタ鍵を取り出し、上記手順を繰り返す。

【0032】一方、復調回路14にて復調された暗号化データ $EDk(Data)$ は、誤り訂正回路15にて誤り訂正処理を受ける。そして、誤り訂正回路15において誤り訂正処理を施された暗号化された $EDK(Data)$ は、復号ユニットCへ伝送される。

【0033】誤り訂正回路15では、誤り訂正処理中に得られる暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置および誤りシンボル値を取り出し、この取り出された誤り位置及び誤りシンボル値を誤りパターン記憶回路16に記憶する。

【0034】そして、誤りパターン記憶回路16に記憶された誤り検出位置および誤り訂正前のシンボル値とから、情報記録媒体に識別情報が存在するか否かを識別情報判定回路17にて調べる。この判定方法について、他の実施の形態とともに、後にまとめて説明する。

【0035】識別情報判定回路17における判定結果を示す制御信号 $CS2$ は、暗号回路18にて先に共有され

た一時暗号鍵Bkを暗号鍵としてEBK(CS2)に暗号化され、復号ユニットCへ伝送される。

【0036】復号ユニットCにおける復号回路39では、受信したEBK(CS2)を一時鍵Bkを復号鍵として復号回路39にて復号し制御信号CS2を得る。

【0037】そして、コピー防止回路40は、復号回路39から出力される制御信号CS2と、例えば、CGMSにおけるコピー管理信号とに基づいて、コピー可能か否かを判定し、コピー不可能であればコピーできないようにする。

【0038】例えば、D/A変換回路38の手前で、タッピングなどの技術を用いてデータを取り、記録したディスクであるならば、誤り訂正回路を通っているため、識別情報は存在しない。その結果、コピー防止回路40によりコピーが防止される。

【0039】すなわち、D/A変換回路38の手前で採取されたデータは、識別情報と入れ替える前のシンボルに変わっている。従って、識別情報は特定位置にはなく、コピーされたディスクであることが判定できる。

【0040】誤り訂正された暗号化されたデータEDk(Data)は、バスインターフェースBを通して復号ユニットCへ送られる。そして、復号ユニットCでは、判定回路35により得られたDkを用いて復号回路36にて暗号化されたデータEDk(Data)を復号する。

【0041】復号されたDataは、伸長回路37にて伸長され、さらにD/A変換回路38にてアナログデータに変換されて、ディスプレイ(図示せず)やアンプを通じてスピーカ(図示せず)により再生される。

【0042】<第2の実施の形態>上述の実施の形態においては、通常の誤り訂正符号の場合を説明した。しかしながら、マルチメディアなどのデジタルデータでは、現在ほとんどが2重符号化誤り訂正符号を用いて誤り訂正符号化されている。そこで、次に2重符号化誤り訂正の場合の実施形態について説明する。

【0043】図4に、一般的な積符号の符号化および復号化の流れを示す。

【0044】積符号の場合、二次元的にシンボルを配列することによって構成される。図4のごとく、まず行方向に誤り訂正符号化されて、内符号ができる。

【0045】次に、列方向に誤り訂正符号化されて外符号ができる。そして、これを伝送する。受信された積符号は、外符号が復号され、次に内符号が復号される。このとき、外符号の復号の際に誤り訂正不可能と判定された場合は、その列すべてにフラグと呼ばれるビットをたてて、誤りの存在を示す。内符号の復号の際に、そのフラグが立っているシンボルは消失したものとして訂正することで、訂正能力を増すことができる。これが消失訂正である。

【0046】図5は、積符号を使用した場合の情報記録媒体の製造手順を示す図である。

【0047】これまでと同様に、アナログ・コンテンツはA/D変換回路51にてデジタル情報に変換される。そして、内符号符号化回路52にて誤り訂正符号化される。そして、識別情報が規則に従って識別情報挿入回路53にてデジタルデータのうちの所定のシンボルと入れ替えられる。

【0048】次に、内符号により誤り訂正符号化され、識別情報が挿入されたデジタルデータは、外符号符号化回路54にて符号化され、その後、変調回路55により変調処理を受け、情報記録媒体に記録される。ここで、識別情報の挿入の方法については後述する。

【0049】図6は、本発明の第2の実施の形態に係るコピー防止装置を示す図である。なお、図6において、図3と同一部分には同一符号を付し、その説明を省略する。

【0050】同図において、一時鍵&データ暗号鍵判定部61は、図3に示した復調/誤り訂正回路12、暗号回路13、鍵共有21、復号回路32、鍵メモリ31、復号回路33、34及び判定回路35を1つのセクションで表したものである。

【0051】DVDディスク11から、暗号化された鍵情報であるEMki(Dk)とEDk(Dk)が読み出される。そして、図3において説明した場合と同様に、一時鍵生成とデータ暗号鍵の判定が一時鍵&データ暗号鍵判定部61にて行われ、一時鍵Bkとデータ暗号鍵Dkが得られる。

【0052】DVDディスク11に記録された暗号化データEDk(Data)は、復調回路14により復調され、さらに外符号誤り訂正回路62により外符号の誤り訂正処理を受ける。

【0053】このとき、外符号誤り訂正処理が済んだデータは、識別情報検出回路64にて識別情報メモリ63に記録された識別情報のパターンと比較され、識別情報DIが取り出される。

【0054】そして、識別情報判定回路65にてオリジナルディスクかコピーであるかを判定して、制御信号CS2を出力する。出力された制御信号CS2は、一時鍵Bkを暗号鍵として暗号回路18にて暗号化され、この暗号化されたEBk(CS2)は復号ユニットCに伝送される。

【0055】伝送されたEBk(CS2)は、一時鍵Bkを復号鍵として復号回路39により復号され制御信号CS2が得られる。コピー防止回路40は、制御信号CS2とコピー管理信号とから、コピー可能か否かを判定し、コピー不可能であればコピーできないようにする。

【0056】一方、外符号誤り訂正回路62により外符号誤り訂正処理を受けた暗号化データは、識別情報を抽出された後、そのシンボルにフラグが立てられる。そして、このフラグは、内符号誤り訂正回路66における内符号誤り訂正処理にて消失訂正を受ける。

【0057】こうして誤り訂正された暗号化データは、復号ユニットCに伝送される。伝送された暗号化データ

は、復号回路36にて復号され、伸長回路37にて伸長され、さらにD/A変換回路38にてアナログデータに変換されて、ディスプレイ（図示せず）やスピーカ（図示せず）を通して再生される。

【0058】例えば、D/A変換回路の手前で、タッピングなどの技術を用いてデータを取り、記録したディスクであるならば、誤り訂正回路62、66を通っているので、識別情報は存在しない。

【0059】すなわち識別情報と入れ替える前のシンボルに変わっているはずである。従って、識別情報は特定位置にはなく、コピーされたディスクであることが判定できる。

【0060】＜第3の実施の形態＞上述の第2の実施形態では、外符号復号において識別情報を取り出す方式になっている。このため、誤り訂正符号の信頼度が低い（誤訂正確率や訂正不能確率が高い）という問題がある。

【0061】また、識別情報をメモリに予め記録されているパターンとの比較により取り出すという方式であるため、誤訂正した場合や訂正不能であった場合に、識別情報を誤検出してしまう確率が高くなるという問題がある。

【0062】そこで上記問題点を解決する、積符号を利用した場合の第3の実施形態について説明する。

【0063】積符号を用いた場合の情報記録媒体の制作手順を図7に示す。図5と異なるのは、識別情報挿入回路53の位置である。

【0064】アナログ・コンテンツは、A/D変換回路51にてデジタル情報に変換される。そして、内符号符号化回路52にて誤り訂正符号化され、次に外符号符号化回路54にて符号化される。

【0065】そして、識別情報が規則に従って識別情報挿入回路53にて入れ替えられ、変調回路55で変調処理を受け、情報記録媒体に記録される。ここで、識別情報の挿入の方法について後述する。

【0066】次に、図7に示した方法により制作されたDVDディスクを再生するコピー防止装置について説明する。

【0067】図8は、本発明の第3の実施の形態に係るコピー防止装置を示す図である。なお、図6と同一部分には同一符号を付し、その説明を省略する。

【0068】DVDディスク11から、暗号化された鍵情報であるEMki(Dk)とEDk(Dk)が読み出される。そして、一時鍵生成とデータ暗号鍵の判定が一時鍵&データ暗号鍵判定部61にて行われ、一時鍵Bkとデータ暗号鍵Dkが得られる。

【0069】DVDディスク11に記録された暗号化データEDk(Data)は、復調回路14により復調され、さらに外符号誤り訂正回路71により外符号誤り訂正処理を受ける。

【0070】また、外符号誤り訂正回路71は、誤り訂正処理時に得られる誤り位置情報と訂正前の誤りシンボル値を誤りパターン記憶回路73へ送る。

【0071】次に、外符号誤り訂正処理が行われたデジタルデータに対して内符号誤り訂正回路72にて内符号誤り訂正処理が行われ、外符号誤り訂正と同様に、内符号誤り訂正回路72は内符号誤り訂正処理において得られる誤り位置情報と訂正前の誤りシンボル値を誤りパターン記憶回路73へ送る。

【0072】こうして誤り訂正の結果得られた誤り位置情報と訂正前の誤りシンボル値と、識別情報メモリ74からの識別情報とから、識別情報検出回路75にて識別情報が検出される。

【0073】そして、識別情報判定回路76にて識別情報が存在するか否かの判定が行われ、この判定結果を示す制御信号CS2が出力される。なお、識別情報判定回路76における判定の方法について後述する。

【0074】制御信号CS2は、一時鍵Bkを暗号鍵として暗号回路18にて暗号化されて復号ユニットCへ伝送される。暗号化された制御信号EDK(CS2)は、復号回路39にて復号され制御信号CS2が取り出され、コピー防止回路40に出力される。

【0075】また、誤り訂正処理された暗号化されたデータEDk(Data)は、復号ユニットCへ伝送され、伝送されたEDk(Data)は、一時鍵生成&データ暗号鍵判定部61にて得られたDkを用いて、復号回路36にてEDk(Data)を復号する。続いて、伸長回路812にて圧縮されたデータが伸長され、さらにD/A変換回路38にてアナログデータに変換されて、ディスプレイ（図示せず）やスピーカ（図示せず）を通して再生される。

【0076】例えば、D/A変換回路38の手前で、タッピングなどの技術を用いてデータを取り、記録したディスクであるならば、誤り訂正回路を通っているので、識別情報は存在しない。

【0077】すなわち、識別情報は、識別情報と入れ替える前のシンボルに変わっているはずである。従って、識別情報は特定位置にはなく、コピーされたディスクであることが判定できる。

【0078】こうして得られた制御信号CS2をもとに、コピー防止回路40は、制御信号CS2とコピー管理信号（図示せず）とから、コピー可能か否かを判定し、コピー不可能であればコピーできないようにする。

【0079】＜第4の実施の形態＞第3の実施の形態においては、誤り訂正処理を終えた後に識別情報を取り出すコピー防止装置を示した。ここでは、第4の実施形態として、誤り訂正前に識別情報を取り出すコピー防止装置を示す。

【0080】図9は、本発明の第4の実施の形態に係るコピー防止装置を示す図である。同図において、図8と同一部分には、同一符号を付し、その説明を省略する。

【0081】DVD ディスク11から、鍵情報であるEHki (Dk)とEDk(Dk)が読み出される。そして、一時鍵生成とデータ暗号鍵の判定が一時鍵&データ暗号鍵判定部61にて行われ、一時鍵Bkとデータ暗号鍵Dkが得られる。

【0082】DVD ディスク11に記録された暗号化されたデータEDk(Data)は復調回路14により復調される。復調された暗号化データは、例えば積符号ブロック単位に識別情報メモリ81に記録されている識別情報とのパターン比較が識別情報検出回路82にて行われる。

【0083】ここで識別情報が検出されれば、識別情報DIを暗号回路83にて一時鍵Bkで暗号化し復号ユニットCへ送る。

【0084】復号ユニットCにおける復号回路86では、一時鍵BKを復号鍵として暗号回路83で暗号化された識別情報DIを復号し、識別情報判定回路87へ送る。識別情報判定回路87は、識別情報DIに基づいてオリジナルであるかコピーされたディスクであるかを判定し、この判定結果を示す制御信号CS2を出力する。この判定方法については後述する。

【0085】コピー防止回路40は、制御信号CS2とコピー管理信号とから、コピー可能か否かを判定し、コピー不可能であればコピーできないようにする。この様に、識別情報を復号ユニットCへ暗号化して送り、復号ユニット側で判定することにより、識別情報から制御信号がどのようにして出力されるかを、ディスク・ドライブ制作会社から隠蔽することが可能となる。

【0086】復調された暗号化されたデータEDk(Data)は、外符号誤り訂正回路84、内符号誤り訂正回路85により、それぞれ誤り訂正処理を受け、復号ユニットCへ伝送される。

【0087】伝送されたEDk(Data)は、既に得られたDkを用いて、復号回路36にて復号される。そして、伸長回路37にて圧縮されたデータが伸長され、さらにD/A変換回路38にてアナログデータに変換されて、ディスプレイ(図示せず)やスピーカ(図示せず)を通して再生される。

【0088】例えば、D/A変換回路38の手前で、タッピングなどの技術を用いてデータを取り、記録したディスクであるならば、誤り訂正回路84、85を通っているので、識別情報は存在しない。

【0089】すなわち、識別情報は、識別情報と入れ替える前のシンボルに変わっているはずである。従って、識別情報は特定位置ではなく、コピーされたディスクであることが判定できる。

【0090】<積符号の場合の識別情報の挿入方法>次に、積符号の場合の識別情報の挿入方法について説明する。ここで、識別情報は1シンボルでも複数シンボルでも構わない。複数シンボルである場合は、予め定められた異なるシンボルにしても構わない。

【0091】まず、最も簡単な積符号の特定位置に識別

情報を挿入する場合について説明する。

【0092】図5においては、ある1シンボルを識別情報シンボルとしている。識別情報シンボルとしては、複数存在しても構わない。これまで説明したように、メモリ内に識別情報シンボルを登録しておき、どの識別情報シンボルかを特定すればよいだけである。

【0093】図10の場合、積符号のi番目の列のシンボルが全て識別情報であることが予め判明しているため、外符号の復号処理にてi番目の復号は行わず、フラグを立てるだけの処理にしても構わない。このような場合、内符号の復号処理ではi番目のシンボルは、全て消失シンボルとして扱われることになる。

【0094】逆にある特定の行が全て識別情報であってもよい。この場合は、外符号で誤り訂正が行われてしまうため、例えば図8に示したコピー防止装置のごとく誤り位置と誤りシンボル情報を記憶しておき、識別情報メモリに登録されている識別情報との一致を調べるか、図9に示したコピー防止装置のごとく誤り訂正前に積符号ブロック単位に識別情報シンボルとのパターン比較を行うこととなる。

【0095】次に、常に第i番目のシンボルに特定する必要はなく第j行は第i列というようなルールに従って挿入する方法について説明する。

【0096】図11に示すように、外符号の誤り訂正能力未達のシンボル数だけ、例えば外符号が5シンボル以上誤り訂正可能である場合に、第j、k、1行の第i列に識別情報を挿入する(ここでは、積符号ブロック内に3シンボル挿入される)ようにしておく。

【0097】識別情報検出時に、後述する識別情報判定処理を行うことにより、オリジナルかコピーかを判定することが可能となる。

【0098】また、図6に示したコピー防止装置の場合には、識別情報に誤りが発生した場合にも外符号の復号処理で誤り訂正が可能で、識別情報が得られなくなる場合を減らすことが可能となる。しかし、この場合は外符号の情報部にのみ挿入し、挿入後に外符号符号化を行う必要がある。

【0099】上記2つの識別情報挿入方法の場合、特定位置に識別情報を埋め込んでいるため、識別情報挿入位置が漏洩した場合、不正コピーが可能となる場合がある。

【0100】そこで、次に、識別情報の埋め込み位置を変化させる方法を説明する。

【0101】例えば、図12のごとく、ある複数シンボルのパターンを識別情報とする場合に、積符号ブロック単位ごとに、決められた個数のシンボルパターンを挿入する。識別情報を取り出すときに、積符号ブロックの中で得られたシンボルパターンの個数を計算し、その個数がある閾値以上になればオリジナルであると判定するようにしてもよい。

【0102】次に、複数のシンボルパターンによる識別情報の挿入方法について説明する。例えば、図13に示すように、積符号のブロックに複数のシンボルパターンを挿入しておき、検出する際に予め登録された識別情報シンボルパターンと照合するようにする。

【0103】このシンボルパターンは、それぞれが異なるシンボルパターンでも構わないし、同じシンボルが n シンボル（例えば $n=5$ ）続くパターンにしても構わない。この場合、識別情報の抽出は、あるシンボルが連続して n シンボル現れたら、それは識別信号であると判定すれば良い。

【0104】この識別信号の検出には、誤り訂正前に検出を行う図9の方法や、内符号誤り訂正前に検出を行う図6の方法も可能であるが、位置が変化するために誤り位置情報が正確な図8の方法、すなわち誤り位置情報と誤りシンボル情報とから識別信号を検出する方法が好ましい。

【0105】また、前記積符号に識別情報としてのシンボルを挿入する位置は、それぞれが重ならないように異なる位置に挿入する必要がある。

【0106】＜識別情報の判定方法＞次に、識別情報の判定方法について説明する。

【0107】図14は、識別情報の判定方法を説明するためのフローチャートである。

【0108】図14に示すように、例えば積符号ブロック単位で登録された識別情報がいくつ検出されたかを計算し（step1～step3）、予め設定された閾値と比較する（step4）ことで、オリジナルかコピーかを判定することが可能となる。上記方法は、シンボルパターンをチェックする方法である。

【0109】次に識別情報の位置情報のみを利用してオリジナルかコピーであるかを判定する方法について説明する。

【0110】例えば、図15のように、各行に特定シンボルパターンを挿入しておく。そして、識別情報抽出の際に、何番目のシンボル位置であるかを、各行について検出する。

【0111】そして、それら位置情報をパラメータとして、一方向性関数（図における関数 g ）に通す。一方向性関数は、異なる入力パラメータに対して、異なる出力をだす。このため、識別情報が挿入された位置情報を複数定めておき、その位置情報から得られる一方向性関数の出力結果 r と照合することで、オリジナルなものであるかコピーであるかを判定することが可能となる。

【0112】次に、他の識別情報の判定方法について説明する。

【0113】上記判定方法では、メモリや一方向性関数の結果を照合する必要があった。

【0114】そこで、識別情報を予め決めておき、各行に1シンボルだけ挿入する。識別情報抽出の際に、その

位置情報をパラメータとして所定の関数 g_0 に入力する。この関数 g_0 の出力 r を一方向関数 H_0 に入力する。このとき、 r がある値であれば、すなわち、特定の位置情報をパラメータとした場合は、関数 H_0 の出力がすべて同じ c になるようにしておく。

【0115】こうすることで、関数 H_0 の出力が c であるか否かでオリジナルかコピーであるか判定できる。よって、メモリも必要なくなり、処理時間を短縮することが可能となる。

【0116】＜第5の実施の形態＞これまでの実施形態は、識別情報の位置情報が固定であるか、可変であってもその位置が真に識別情報のシンボル位置であるのか、を確定することが困難で、識別情報の個数などによる統計処理により処理する方法であった。

【0117】そこで、現在新しい著作権保護技術として注目されている電子透かし技術を利用した方法について説明する。

【0118】図17は、本発明の第5の実施の形態に係るコピー防止装置にて使用される情報記録媒体の制作過程を示す図である。

【0119】本実施形態では、識別情報を埋め込むための位置情報をコンテンツに電子透かしとして埋め込むものとする。電子透かしは特徴として、除去しにくく、また取り出しにくいという性質を持つためである。電子透かしについては、「画像深層暗号—手法と応用—」松井著、森北出版株式会社に詳しい。

【0120】さて、アナログ・コンテンツは、A/D変換回路91にてデジタル情報に変換される。識別情報のための位置情報は電子透かし情報埋め込み回路92にてコンテンツに埋め込まれる。

【0121】図17では、A/D変換回路91と電子透かし情報埋め込み回路92とが別々に示してあるが、多くの透かし埋め込み技術は量子化する際に透かし情報を埋め込むため、A/D変換回路に透かし情報埋め込み回路を組み込んでおくことが多い。図17では、説明しやすいように別にした。

【0122】識別情報のための位置情報が埋め込まれたコンテンツは、誤り訂正符号化回路93にて誤り訂正符号化される。そして、識別情報が識別情報のための位置情報に従って、識別情報挿入回路94にて一部のコンテンツと入れ替えられる。そして、識別情報が挿入されたコンテンツが情報記録媒体に記録される。

【0123】上記手法を用いれば、識別情報をその都度変化させ、かつ電子透かし技術を用いて位置情報を記録するため、不正に識別情報を埋め込んであるシンボル位置を特定することは困難となる。

【0124】例えば図18のごとく、識別情報を埋め込むための位置情報に従って、識別情報を i 行目 u 列のシンボル、 j 行目 s 列、 k 行目 t 列に埋め込む、ということになる。もちろん場合により、識別情報がデータ部に

のみ埋め込まれる場合や、パリティ部にのみ埋め込まれる場合がある。ただし、識別情報は同じシンボル位置に挿入することがないように気をつける必要がある。

【0125】次に、識別情報の位置を変化させた場合の情報記録媒体の再生について説明する。

【0126】図19は、本発明の第5の実施の形態に係るコピー防止装置を示す図である。なお、図9と同一部分には、同一符号を付し、その説明を省略する。

【0127】DVD ディスク11から、暗号化された鍵情報であるEMki(Dk)とEDk(Dk)が読み出される。そして、これまでと同様に一時鍵生成とデータ暗号鍵の判定が一時鍵&データ暗号鍵判定部61にて行われ、一時鍵Bkとデータ暗号鍵Dkが得られる。

【0128】復調回路14にて復調処理を受けた暗号化データEDk(Data)は、誤り訂正回路91により誤り訂正処理を受ける。なお、本実施形態では、誤り訂正回路91において内符号、外符号ともに誤り訂正符号化されるものとする。

【0129】暗号化データEDk(Data)の誤り訂正処理中に得られた誤り位置情報と誤りシンボル値とから、誤りパターンが得られる。この誤りパターンを誤りパターン記憶回路92にて記憶する。

【0130】一方、誤り訂正回路91にて誤り訂正が行われた暗号化データEDk(Data)は、バスインターフェースBを通じて、復号ユニットCへ伝送される。伝送された暗号化データEDk(Data)は、一時鍵生成&データ暗号鍵判定部61にて得られたデータ暗号鍵Dkを用いて復号回路36にて復号される。

【0131】復号回路36において得られたDataには識別情報の埋め込み位置情報が透かし情報として埋め込まれている。復号されたDataは電子透かし情報抽出回路101に入力され、識別情報の位置情報が抽出される。抽出された識別情報の位置情報locは、一時鍵Bkを復号鍵として復号回路102にて復号され、ディスク・ドライブAへ伝送される。

【0132】ディスク・ドライブAにおける暗号化回路94においては、識別情報の位置情報locが一時鍵Bkを暗号鍵として暗号回路94にて暗号化され、識別情報の位置情報locが取り出される。

【0133】そこで、先の誤りパターン記憶回路92に記録された誤りパターンと、識別情報の位置情報locとから、識別情報抽出回路93にて識別情報DIが抽出される。この識別情報DIから識別情報判定回路95にてディスクがオリジナルかコピーかが判定され、判定結果を示す制御信号CS2が出力される。

【0134】出力された制御信号CS2は、暗号回路96にて一時鍵Bkを暗号鍵として暗号化され、復号ユニットCへ伝送される。復号ユニットCでは、復号回路103にて一時鍵Bkを復号鍵として復号し、制御信号CS2を得る。

【0135】例えば、D/A変換回路の手前で、タッピングなどの技術を用いてデータを取り、記録したディスクであるならば、誤り訂正回路91を通っているので、識別情報は存在しない。

【0136】すなわち、識別情報は、識別情報と入れ替える前のシンボルに変わっているはずである。従って、識別情報は特定位置にはなく、コピーされたディスクであることが判定できる。

【0137】このように、識別情報判定回路95は、コピーされたか、オリジナルであるかを判定し、コピー可能か不可能かを示す制御信号CS2を出力する。コピー防止回路40は、制御信号CS2を利用して、オリジナル・ディスクとコピー管理信号とから、コピー可能か否かを判定し、コピー不可能であればコピーできないようにする。

【0138】復号回路36にて復号された暗号化データDataは、伸長回路37にて圧縮されたデータが伸長され、さらにD/A変換回路38にてアナログデータに変換されて、ディスプレイやスピーカ(図示せず)を通して再生される。

【0139】この様に透かし情報を利用することにより、識別情報の位置情報を可変にし、かつ秘密裏に積符号内に識別情報を埋め込むことが可能となる。

【0140】<制御信号を安全に伝送する方法>次に、制御信号CS2を安全に伝送する方法について述べる。

【0141】制御信号CS2はオリジナルかコピーかを示す信号であり、少なくとも1ビットあれば済む。例えば、“0”であればコピー、“1”であればオリジナル、という設定が考えられる。これは逆でも構わない。

【0142】このように少ないビットを暗号化した場合、元のデータ(暗号学上では明文)を長い鍵で暗号化しても、解読されやすい、という性質がある。

【0143】従って、バス上を一時鍵で暗号化したとしても、解読されてしまう恐れがある。ここで、制御信号CS2を安全に伝送する方法について、図20を用いて説明する。

【0144】図20において、Aはディスク・ドライブ、Bはバスインターフェース、Cは復号ユニットである。なお、図20では、必要な部分のみを図示している。

【0145】これまで示してきた実施形態において、識別情報DIが取り出されたものとする。この識別情報DIは、識別情報判定回路111にて判定され、判定結果を示す制御信号CS2が出力される。

【0146】一方、乱数生成回路112にて乱数Rが生成され制御信号CS2との排他論理和演算が行われる。また、乱数Rは暗号回路115にて一時鍵Bkにて暗号化され、暗号化された乱数EBK(R)が復号ユニットCにおける復号回路122に伝送される。

【0147】また乱数Rと制御信号CS2との排他論理和

R' も同様に暗号回路 1 1 4 にて一時鍵 Bk で暗号化され、暗号化された排他的論理和 R' が復号ユニット C の復号回路 1 2 1 に伝送される。

【0148】復号ユニット C では、伝送された暗号化された乱数 EBK(R) を復号回路 1 2 2 において一時鍵 Bk で復号し、復号回路 1 2 1 において暗号化された排他論理和の結果である EBK(R') を一時鍵 Bk で復号する。

【0149】そして、乱数 R と排他論理和の結果である R' を得て、この 2 つの排他論理和演算を行うことで、制御信号 CS2 を取り出すことができる。この乱数のビット長は、暗号化を行うときの入力ビット長と同じにしておけば良い。

【0150】ここで、図 20 における乱数生成回路を使用せず、一時鍵生成で使用する乱数を使用しても良い。この一時鍵の生成で使用する乱数は、ディスク・ドライブ、復号ユニットの両方で共有される乱数であるので、図 20 のような乱数を暗号化して送る手順を省くことができる。

【0151】また、乱数生成回路により生成される乱数が暗号などで使用される条件、任意の長さでの全系列の等頻度性、無相関性、長周期性、非線型性、予測不可能性、といった諸条件を満足するものであるならば、暗号回路 1 1 4、復号回路 1 2 1 を省略することもでき、処理手順や回路を簡単にすることができる。

【0152】＜識別情報の特定＞次に、識別情報を特定するための方法について説明する。

【0153】ここで述べる識別情報を特定するための方法は、DVD における CSS(Content Scramble System) というシステムを利用した方法である。CSS については、前述した「DVD、パソコン載る」日経エレクトロニクス、1997.8.18(no.696)、p.110-120 に説明されている。

【0154】文献に依れば、DVD ディスクのリードイン領域という特殊な領域（論理ファイル・システムからはアクセスできない領域）があり、そこに暗号化された鍵情報を格納する領域がある。

【0155】そこで、この暗号化された鍵情報 EMki(Dk), EDk(Dk) を利用して識別情報の位置情報を特定する方法を図 21 に示す。なお、図 21 では、ディスク・ドライブの必要な部分のみを図示している。

【0156】さて、DVD ディスク 1 3 1 から暗号化された鍵情報 EMki(Dk), EDk(Dk) が読み出され、ハッシュ関数（データを圧縮する関数）1 3 5 を用いて圧縮される。この圧縮された鍵情報 EMki(Dk), EDk(Dk) が識別情報の位置情報 loc となる。

【0157】従って、この方法を使用した場合には、ディスク内の全ての積符号ブロックにおいて、識別情報の挿入位置が固定となる。ただし、ディスクが異なれば識別情報の挿入位置を異なる位置にすることも可能である。

【0158】従って、識別情報を挿入する位置は、コン

テンツ・データを誤り訂正符号化して、識別情報を挿入する前に、この記録するディスクの鍵情報 EMki(Dk), EDk(Dk) とハッシュ関数とを用いて予め計算しておき挿入する必要がある。このときハッシュ関数は、鍵情報 EMki(Dk), EDk(Dk) を入力したときに、必ず積符号ブロックの誤り訂正符号長さ以下となる必要がある。

【0159】ハッシュ関数 1 3 5 により変換された暗号化された鍵情報 EMki(Dk), EDk(Dk) は、識別情報の位置情報 loc となる。一方、読み出された暗号化データ EDk(Data) は、復調回路 1 3 2 にて復調処理を受け、誤り訂正回路 1 3 3 により誤り訂正処理を受ける。なお、誤り訂正回路 1 3 3 において内符号、外符号ともに誤り訂正されるものとする。

【0160】暗号化されたデータ EDk(Data) の誤り訂正処理中に得られた誤り位置情報と誤りシンボル値とから、誤りパターンが得られる。この誤りパターンは、誤りパターン記憶回路 1 3 4 にて記憶される。

【0161】そして、識別情報の位置情報 loc と、誤りパターン記憶回路 1 3 4 に記憶された誤りパターンとから、識別情報 DI が抽出される。

【0162】＜識別情報の訂正＞次に、識別情報そのものが誤り訂正符号である場合について説明する。

【0163】すなわち、上述の実施の形態において、識別情報が誤り訂正符号である場合である。

【0164】図 22 は、識別情報に誤り訂正符号を使用した場合の識別情報の判定処理を説明するためのフローチャートである。

【0165】同図に示すように、識別情報が検出される (step 11) と、この検出された識別情報に対して、その誤り訂正能力を使用して誤り訂正が行われる (step 12)。

【0166】そして、次に、この誤り訂正が施された識別情報に対して、識別情報の決定が行われる (step 13)。従って、識別情報に誤り訂正符号を使用した場合には、復調された識別情報自体に誤りが存在していても、その誤り訂正能力を使用して識別情報を訂正するので、より正確に識別情報が存在するか否かを決定することができる。

【0167】

【発明の効果】以上詳記したように、本発明によれば、誤り訂正符号にオリジナルの記録媒体であるのかを示す識別信号を、誤りとして挿入することにより、誤り訂正処理前にその識別情報を抽出することで、オリジナルな記録媒体であるかを判定することが可能となる。

【0168】また、誤り訂正処理を終えれば、識別情報は誤りとして処理されるため、元の正しいシンボルに訂正される。このため、再生処理途中でデータをコピーしたとしても、オリジナルであるための識別情報が失われるため、不正なコピーをした情報記録媒体を役に立たせなくすることが可能となる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態におけるコピー防止装置において使用されるディスクの制作の過程を説明するための図。

【図2】識別情報の挿入方法について説明するための図。

【図3】本発明の第1の実施の形態に係るコピー防止装置を示す図。

【図4】一般的な積符号の符号化および復号化の流れを示す図。

【図5】積符号を使用した場合の情報記録媒体の製造手順を示す図。

【図6】本発明の第2の実施の形態に係るコピー防止装置を示す図。

【図7】本発明の第3の実施の形態に係るコピー防止装置において使用される情報記録媒体の製造方法を示す図。

【図8】本発明の第3の実施の形態に係るコピー防止装置を示す図。

【図9】本発明の第4の実施の形態に係るコピー防止装置を示す図。

【図10】識別情報の挿入方法を説明するための図。

【図11】識別情報の挿入方法を説明するための図。

【図12】識別情報の挿入方法を説明するための図。

【図13】識別情報の挿入方法を説明するための図。

【図14】識別情報の判定方法を説明するためのフローチャート。

【図15】識別情報の挿入方法を説明するための図。

【図16】識別情報の挿入方法を説明するための図。

【図17】本発明の第5の実施の形態に係るコピー防止装置にて使用される情報記録媒体の制作過程を示す図。

【図18】識別情報の挿入方法を説明するための図。

【図19】本発明の第5の実施の形態に係るコピー防止装置を示す図。

【図20】制御信号を安全に伝送する方法を説明するための図。

【図21】鍵情報を利用して識別情報の位置を特定するための方法を説明するための図。

【図22】識別情報に誤り訂正符号を使用した場合の識別情報の判定処理を説明するためのフローチャート。

【符号の説明】

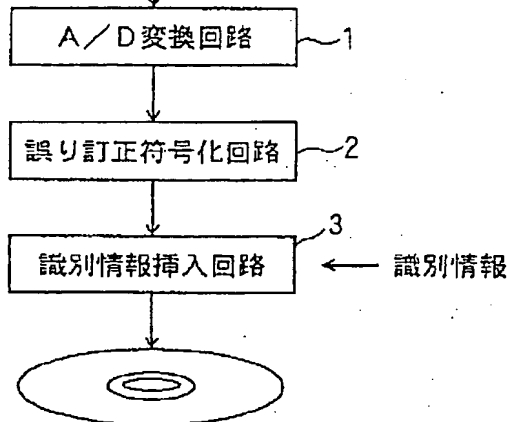
1…A/D 変換回路、
2…誤り訂正符号化回路、
3…識別情報挿入回路、
11…DVD ディスク、
12…復調／誤り訂正回路、

13…暗号化回路、
14…復調回路、
15…誤り訂正回路、
16…誤りパターン記憶回路、
17…識別情報判定回路、
18…暗号回路、
31…鍵メモリ、
32…復号回路、
33…復号回路、
34…復号回路、
35…判定回路、
36…復号回路、
37…伸長回路、
38…D/A 変換回路、
39…復号回路、
40…コピー防止回路、
51…A/D 変換回路、
52…内符号符号化回路、
53…識別情報挿入回路、
54…外符号符号化回路、
55…変調回路、
61…一時鍵&データ暗号鍵判定部、
62…外符号誤り訂正回路、
63…識別情報メモリ、
64…識別情報検出回路、
65…識別情報判定回路、
66…内符号誤り訂正回路、
71…外符号誤り訂正回路、
72…内符号誤り訂正回路、
73…誤りパターン記憶回路、
74…識別情報メモリ、
75…識別情報検出回路、
76…識別情報判定回路、
81…識別情報メモリ、
82…識別情報検出回路、
83…暗号回路、
84…外符号誤り訂正回路、
85…内符号誤り訂正回路、
86…復号回路、
87…識別情報判定回路、
93…識別情報抽出回路、
95…識別情報判定回路、
101…電子すかし情報抽出回路、
111…識別情報判定回路、
112…乱数生成回路。

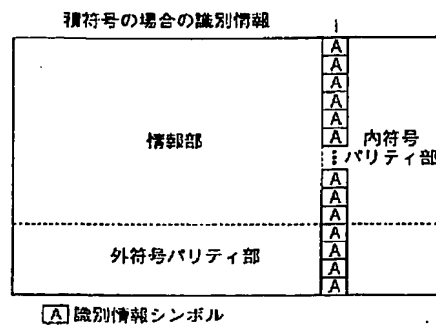
【図1】

ディスク制作 # 1

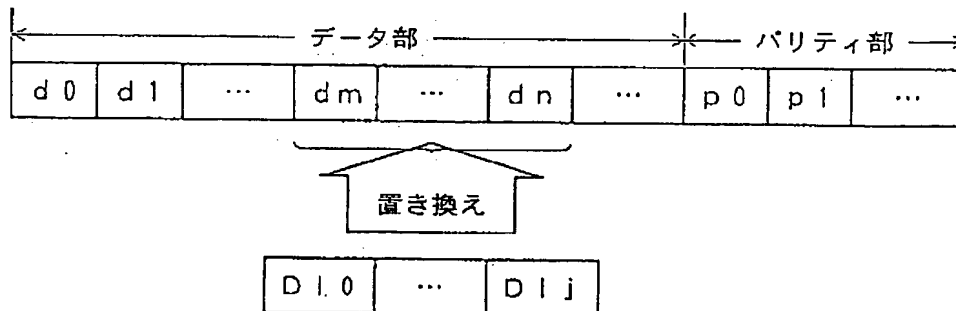
アナログ・コンテンツ



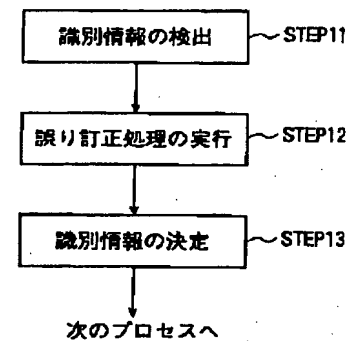
【図10】



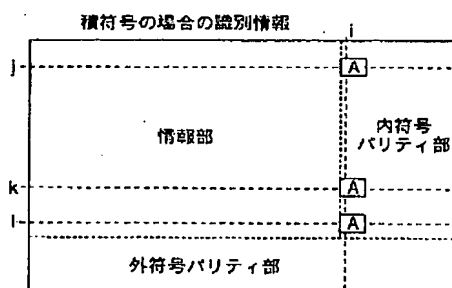
【図2】



【図22】

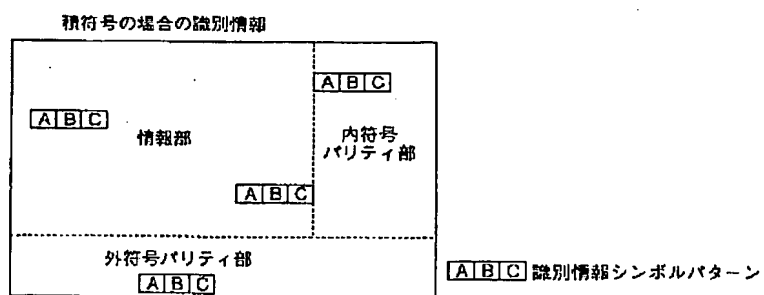


【図11】



外符号は5シンボル以上誤り訂正可能とする

【図12】



ディスク再生#1

鍵共有

復調/誤り訂正回路 12

暗号回路 13

復調回路 14

誤り訂正回路 15

誤りパターン記憶回路 16

識別情報判定回路 17

暗号回路 18

復号回路 32

復号回路 33

復号回路 34

判定回路 35

復号回路 36

伸長回路 37

D/A変換回路 38

コピ-防止回路 40

CS1

CS2

CS

管理番号

ディスク再生#1

鍵共有

復調/誤り訂正回路 12

暗号回路 13

復調回路 14

誤り訂正回路 15

誤りパターン記憶回路 16

識別情報判定回路 17

暗号回路 18

復号回路 32

復号回路 33

復号回路 34

判定回路 35

復号回路 36

伸長回路 37

D/A変換回路 38

コピ-防止回路 40

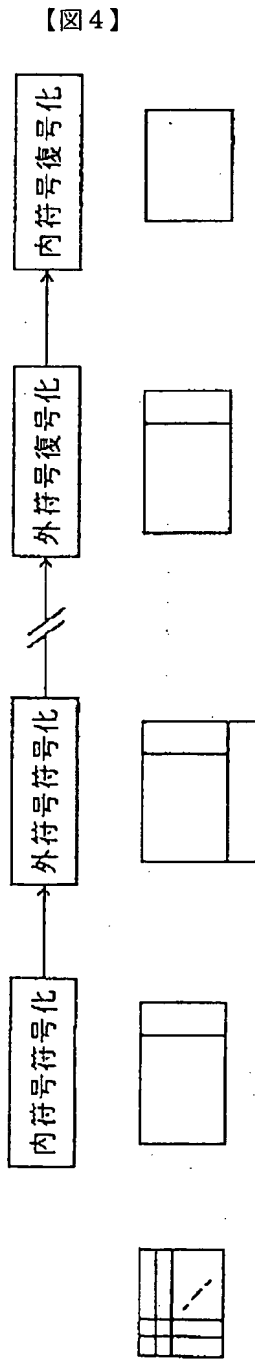
CS1

CS2

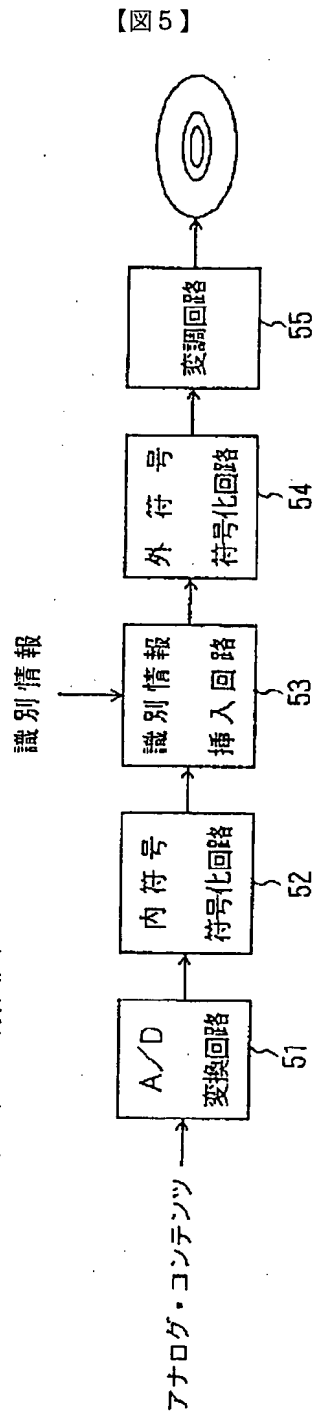
CS

管理番号

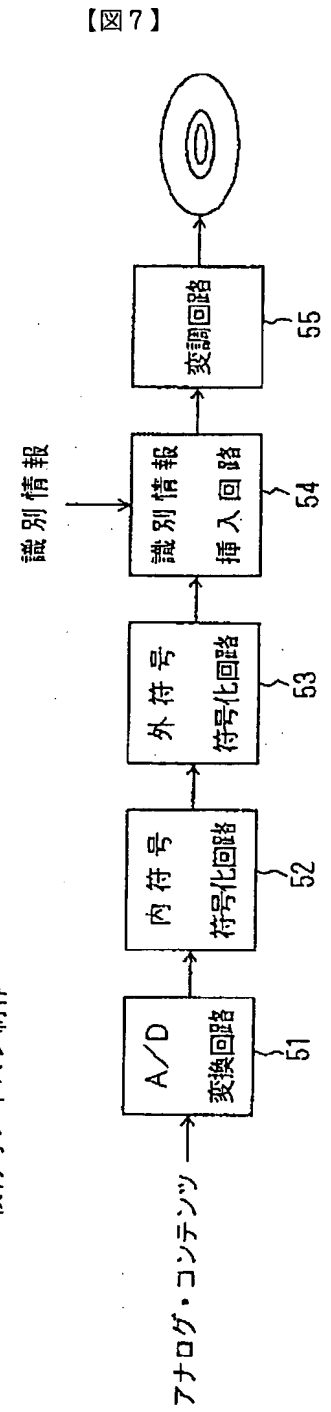
積符号



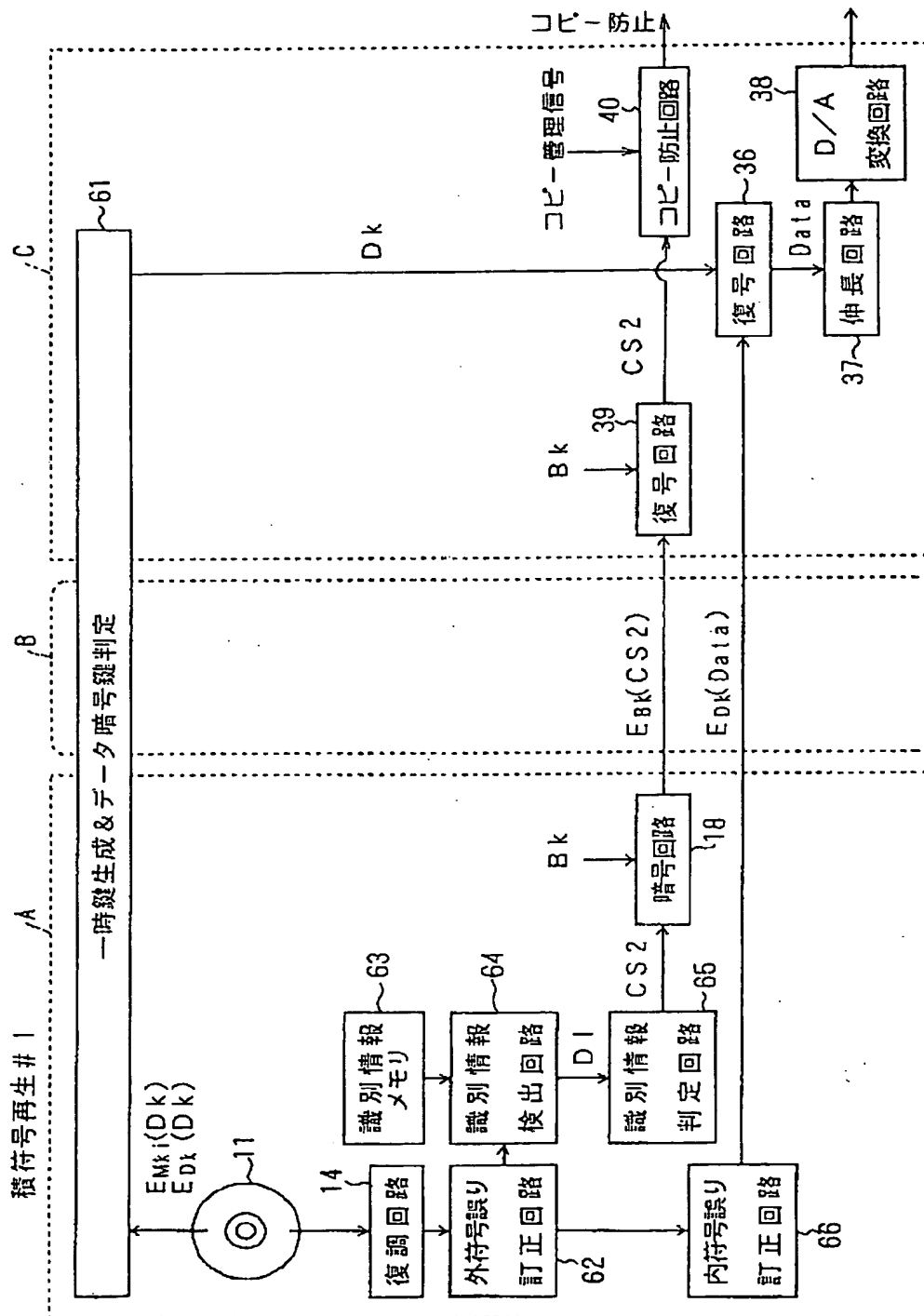
積符号ディスク制作 #1



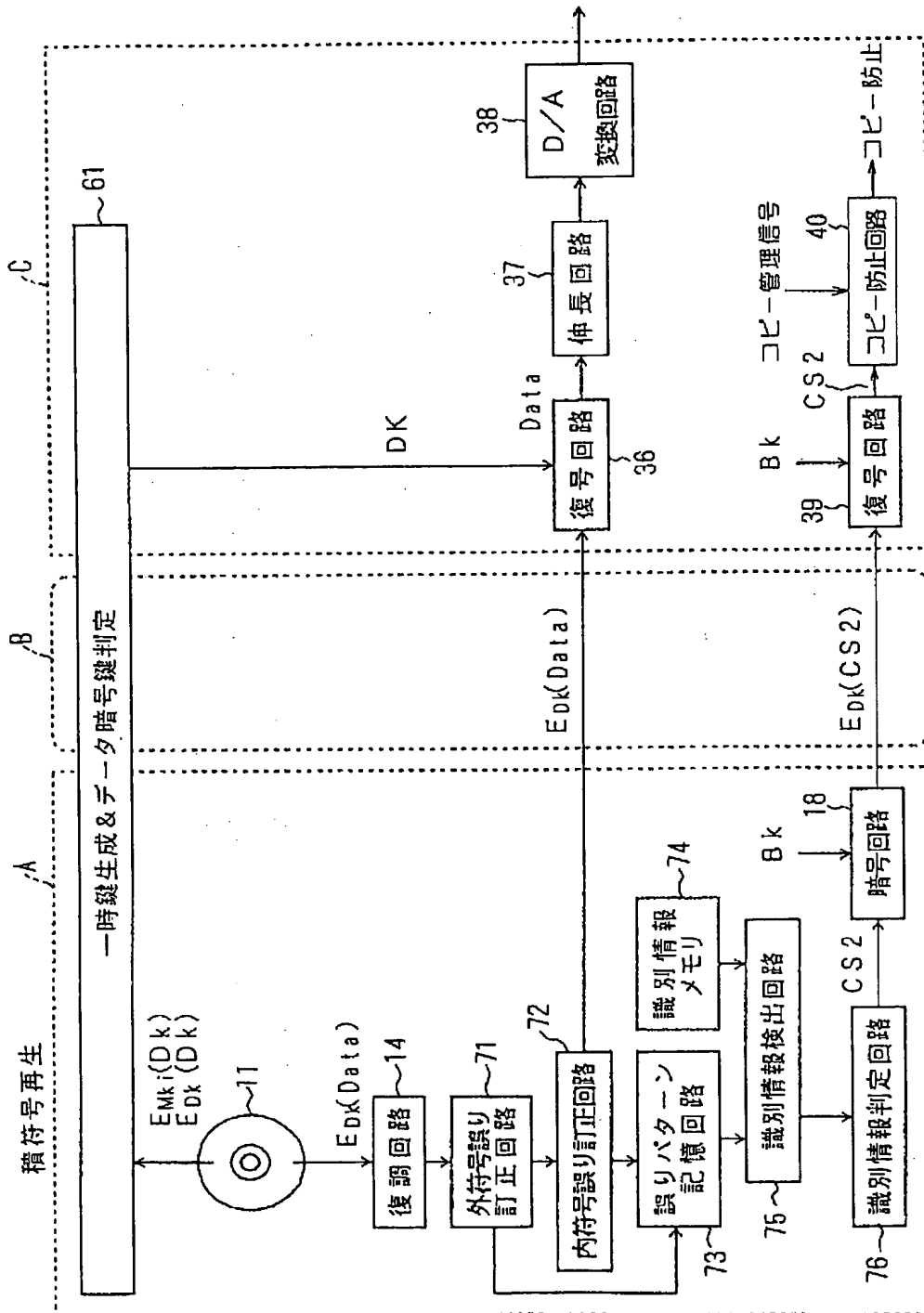
積符号ディスク制作



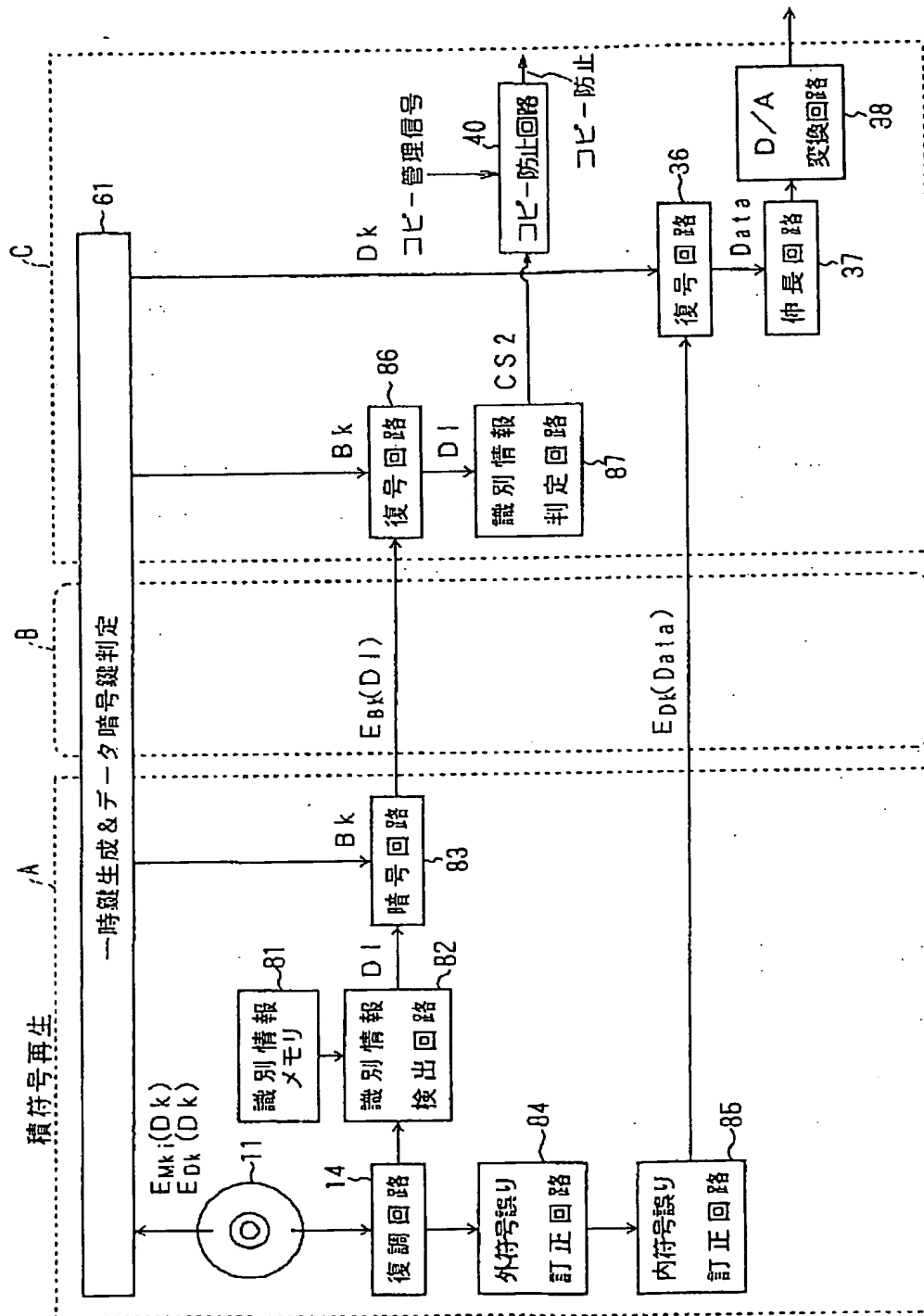
【図6】



【図8】

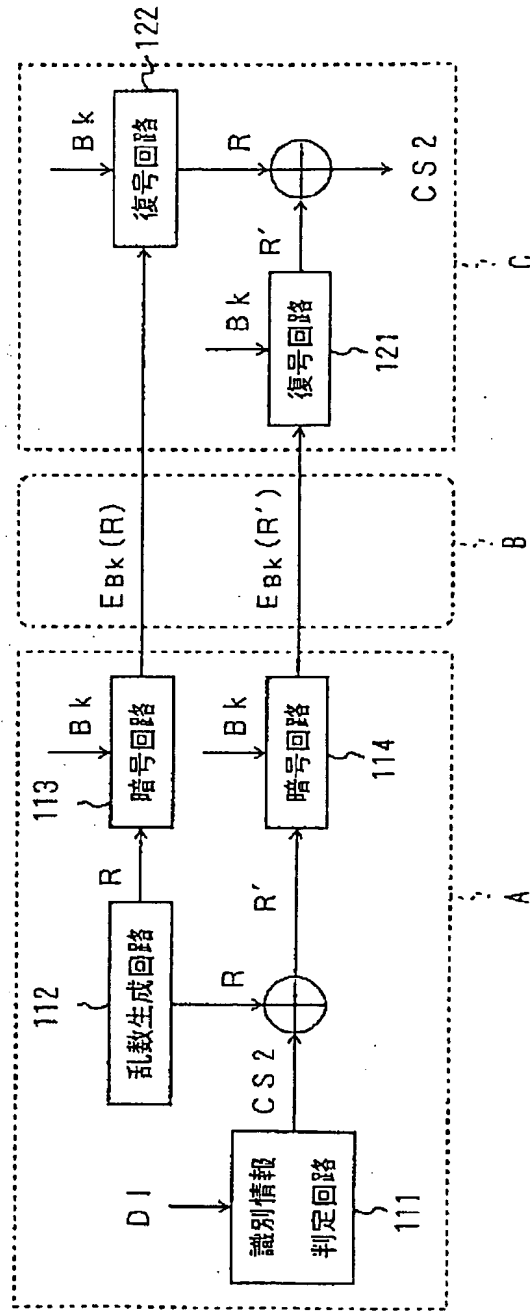


【図9】



【図20】

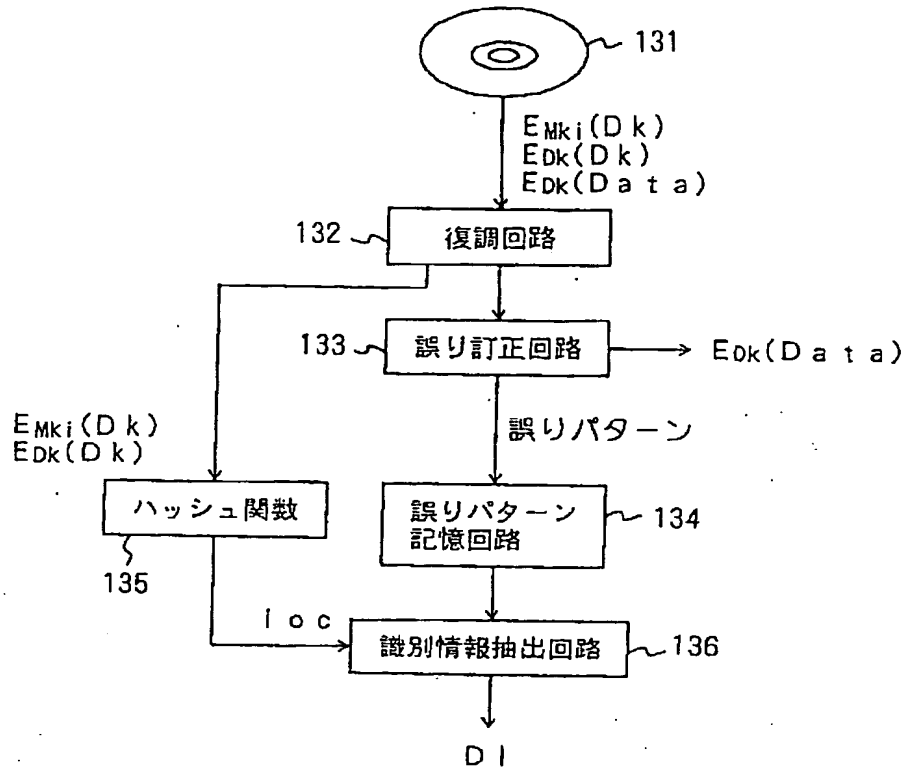
制御信号CS2



⊕ 排他論理和

【図21】

識別情報の位置情報の特定



フロントページの続き

(72)発明者 山田 尚志
 神奈川県川崎市幸区柳町70番地 株式会社
 東芝柳町工場内

(72)発明者 遠藤 謙二郎
 神奈川県川崎市幸区柳町70番地 株式会社
 東芝柳町工場内

THIS PAGE BLANK (USPTO)